

PATENT

C. REMARKS

Claims 1-21 are pending in the present application. Claims 1, 2, 4, 8, 9, 11, 14, 15, and 17 were amended. Claim 21 was newly added. Reconsideration of the claims is respectfully requested.

Applicants would like to thank Examiner Henning for his courtesy in holding the telephone interview of May 5, 2004 between the Examiner and the Applicants' Representative, during which the following issues were discussed.

35 U.S.C. § 112, Second Paragraph

The Examiner has rejected claims 1, 8, and 14 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that Applicants regard as the invention. Specifically, the Examiner rejected claims 1, 8, and 14 for using the words "such as," which fail to make a clear delineation as to whether the subject matter following the words "such as" are true limitations to the claimed subject matter.

In response to the Examiner's rejection, Applicants have amended claims 1, 8, and 14 to use the word "including," rather than "such as," thereby clearly indicating that the recited data includes "identification data and digital certification data" but might also include other data that is not "identification data and digital certification data." Applicants respectfully submit that these amendments obviate the Examiner's rejection under 35 U.S.C. § 112.

Therefore, Applicants respectfully request that the rejection of claims 1, 8, and 14 under 35 U.S.C. § 112, first paragraph be withdrawn.

35 U.S.C. § 102, Anticipation

The Examiner has rejected claims 1-5, 7-12, 14-18, and 20 under 35 U.S.C. § 102 as being anticipated by US 5657390 (ELGAMAL et al.) 1997-8-12. This rejection is respectfully traversed.

With respect to claim 1, which is representative of the other rejected claims, the Examiner stated:

Regarding claim 1, Elgamal disclosed a method of establishing a secure communication path between two computer systems (See Elgamal Col. 3 Paragraph 3) comprising: creating a communication path to exchange data (See Elgamal Col. 6 Line 57 — Col. 7 Line 12) such as identification data

Docket No. AUS920000924US1

Page 8 of 11

Atty Ref. No. IBM-1006

Fiveash et al. - 09/864,110

PATENT

and digital certification data between the two systems (See Elgamal Fig. 4 and Col. 7 Lines 13-40 and Fig. 5 and Col. 8 Line 45 — Col. 10 Line 23); determining, based on the identification data, whether to confirm the digital certification data (See Elgamal Figs. 4-5, Col. 7 Lines 20-65, Col. 10 Lines 3-23, Col. 20 Lines 25-32, Col. 22 Line 56— Col. 23 Line 18); and creating a secure communication path, without confirming the digital certification data if it is determined the digital certification data should not be confirmed (See Elgamal Fig. 5 and corresponding text), or after confirming the digital certification data if it is determined that the digital certification data should be confirmed (See Elgamal Fig. 4 and Corresponding text). [Office Action, March 7, 2005, at 4].

Without necessarily agreeing with the Examiner's position, Applicants have amended independent claims 1, 8, and 14 to specifically recite that a determination is made as to whether to confirm that the digital certification data *has not been revoked*. As stated in Applicants' Summary of their invention, a preferred embodiment of the present invention is directed to improving the performance of a virtual private network by being selective as to when to consult a Certificate Revocation List (CRL) to determine whether a certificate has been revoked or not.

The present invention provides a system and method of dynamically figuring out when to check for revocation the digital certification of a remote system with which a local system is trying to have a secure communication. The method includes creating a non-secure communication path to exchange preliminary data. The preliminary data includes security policies as well as identification data and digital certification data. Once the identification data is received, each computer system checks an internal or endpoints table to see if it should check to see whether the digital certification of the other computer system has been revoked. The internal table is usually set up by a system administrator. If the identification of the other computer system is in the internal table, revocation of the digital certification of the other computer system need not be checked; otherwise, it has to be checked. After deciding not to check for revocation the digital certification of the other computer or after checking for revocation the digital certification of the other computer, a secure communication path or tunnel is created between the two systems to transfer data. [Applicants' Specification, p. 5].

ELGAMAL neither teaches nor suggests this feature. In fact, ELGAMAL not only fails to teach or suggest the claimed feature of determining whether to confirm that digital certification data has not been revoked; ELGAMAL actually fails to make any mention of certificate revocation at all. Hence, the present independent claims, as amended, are not only not anticipated by ELGAMAL, but one of ordinary skill in the art would have no motivation or

PATENT

incentive to modify ELGAMAL to include the claimed feature of determining whether to confirm that a certificate has not been revoked, since the protocol described in ELGAMAL does not even recognize the existence of revoked certificates (and therefore, there is no performance gain to be had by being selective in deciding to confirm the revocation status of a certificate, since, by design, no such confirmations can take place, anyway).

Claims 2-5, 7, 9-12, 15-18, and 20 are dependent claims that depend from independent claims 1, 8, and 14. Applicants have already demonstrated claims 1, 8, and 14 to be in condition for allowance. Applicants respectfully submit that claims 2-5, 7, 9-12, 15-18, and 20 are also allowable, at least by virtue of their dependency on allowable claims. Thus, Applicants respectfully request that the rejection of claim 1-5, 7-12, 14-18, and 20 under 35 U.S.C. § 102 be withdrawn.

35 U.S.C. § 103, Obviousness

The Examiner rejected claims 6, 13, and 19 under 35 U.S.C. § 103 as being obvious in view of ELGAMAL and SCHNEIER (Applied Cryptography). This rejection is respectfully traversed.

Claims 6, 13, and 19 are dependent claims that depend from independent claims 1, 8, and 14. In the previous Section of this Response, Applicants demonstrated claims 1, 8, and 14 to be in condition for allowance. Applicants respectfully submit that claims 6, 13, and 19 are also allowable, at least by virtue of their dependency on allowable claims. Thus, Applicants respectfully request that the rejection of claim 1-5, 7-12, 14-18, and 20 under 35 U.S.C. § 103 be withdrawn.

New Claim 21

Applicants have added an additional independent claim, claim 21, to the present application. This new independent claim incorporates all of the limitations of independent claim 1 and is thus patentable for at least the reasons set forth with respect to claim 1. Further, independent claim 21 contains additional limitations not contained within claim 1, which are not taught or suggested by the cited references. In particular, independent claim 21 recites consulting an internal table identifying all computer systems for which it is not necessary to confirm that certificate data has not been revoked. Independent claim 21 distinguishes this first internal table from a second table, a policy table, which specifies the access methods appropriate

PATENT

to different pairs of endpoint computer systems. ELGAMAL neither teaches nor discloses a computer system having an internal table that specifically identifies whether it is necessary to confirm whether another computer system's certificate has or has not been revoked.

Thus, for these additional reasons, as well as those set forth with regard to independent claim 1, independent claim 21 is patentable over the cited references.

Conclusion

As a result of the foregoing, it is asserted by Applicants that the remaining claims in the Application are in condition for allowance, and Applicants respectfully request allowance of such claims.

Applicants respectfully request that the Examiner contact the Applicants' attorney listed below if the Examiner believes that such a discussion would be helpful in resolving any remaining questions or issues related to this Application.

Respectfully submitted,

By



Joseph T. Van Leeuwen

Attorney for Applicant

Registration No. 44,383

Telephone: (512) 301-6738

Facsimile: (512) 301-6742